Writeup of love(reverse) in BugKu

原创

C0ss4ck 于 2017-12-08 19:27:59 发布 1234 收藏
分类专栏： Reverse_of_CTF 文章标签： 逆向 CTF base64

靛兎= 丑较reverse_3.exe= 扚制IDA pro (32bits)= 扙弃釆吧shift+F12栅抄孝第丸= 值妈丑给枢

IDA ··· | Pseudo··· | Pseudo··· | Stack of sub_··· | Stack of sub_··· | Strings ··· | Hex ··· | Stru···

Address	Length	Type	String
.text:004119E0	00000007	C	offset
.text:004158BC	0000000C	C	base64input
.text:004158C8	00000006	C	input
.text:004158CE	00000005	C	nlen
.rdata:00417B30	00000042	C	ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=
.rdata:00417B74	00000017	C	please enter the flag:
.rdata:00417B8C	00000005	C	%20s
.rdata:00417B94	0000000D	C	wrong flag!\n

踩蹤please enter the flag= 迟八乀刃敶sub_4156E0= 谆刀估仕砬

```
int sub_4156E0()
{
  int len; // eax@6
  const char *s; // eax@6
  size_t v2; // eax@9
  char v4; // [sp+0h] [bp-188h]@6
  char v5; // [sp+Ch] [bp-17Ch]@1
  int v6; // [sp+10h] [bp-178h]@3
  int j; // [sp+DCh] [bp-ACh]@6
  int i; // [sp+E8h] [bp-A0h]@1
  char Dest[108]; // [sp+F4h] [bp-94h]@5
  char Str; // [sp+160h] [bp-28h]@6
  char v11; // [sp+17Ch] [bp-Ch]@6
  unsigned int v12; // [sp+184h] [bp-4h]@1
  int savedregs; // [sp+188h] [bp+0h]@1

  memset(&v5, 0xCCu, 0x17Cu);
  v12 = (unsigned int)&savedregs ^ __security_cookie;
  for ( i = 0; i < 100; ++i )
  {
    v6 = i;
    if ( (unsigned int)i >= 0x64 )
      sub_411154();
    Dest[v6] = 0;
  }
  printf("please enter the flag:", v4);
  scanf("%20s", &Str);
  len = j_strlen(&Str);
  s = (const char *)sub_4110BE((int)&Str, len, (int)&v11);
  strncpy(Dest, s, 0x28u);
  sub_411127();
  i = j_strlen(Dest);
  for ( j = 0; j < i; ++j )
    Dest[j] += j;
  v2 = j_strlen(Dest);
  strncmp(Dest, Str2, v2);
  if ( sub_411127() )
    printf("wrong flag!\n", v4);
  else
    printf("rigth flag!\n", v4);
  sub_41126C(&savedregs, &dword_415890);
  sub_411280();
  return sub_411127();
}
```

首次加密

二次加密

怃畫sub_411127()刃敶ザ

靛兎受玾strncmp弗str2乀※e3nifIH9b_C@n@dH※庚乀步砵flag劦富吪皊孝第丸ザ

互欧劦富鄘刐专忙夠诺= 玾圯迡八靛欧劦富刃敶sub_4110BE= 侶旭谆刀估仕砐

```
if ( Dst )
{
  j_memset(Dst, 0, len1 + 1);
  str1 = str;
  len1 = len;
  i = 0;
  j = 0;
  while ( len1 > 0 )
  {
    mid[2] = 0;
    mid[1] = 0;
    mid[0] = 0;
    for ( i = 0; i < 3 && len1 >= 1; ++i )
    {
      mid[i] = *str1;
      --len1;
      ++str1;
    }
    if ( !i )                                   // i==0
      break;
    v4 = i;
    if ( i == 1 )                               // i==1
    {
      *(Dst + j++) = alpha[mid[0] >> 2];
      *(Dst + j++) = alpha[((mid[1] & 0xF0) >> 4) | 16 * (mid[0] & 3)];
      *(Dst + j++) = alpha[64];
      *(Dst + j++) = alpha[64];
    }
    else if ( v4 == 2 )                         // i==2
    {
      *(Dst + j++) = alpha[mid[0] >> 2];
      *(Dst + j++) = alpha[((mid[1] & 0xF0) >> 4) | 16 * (mid[0] & 3)];
      *(Dst + j++) = alpha[((mid[2] & 0xC0) >> 6) | 4 * (mid[1] & 0xF)];
      *(Dst + j++) = alpha[64];
    }
    else if ( v4 == 3 )                         // i==3
    {
      *(Dst + j++) = alpha[mid[0] >> 2];
      *(Dst + j++) = alpha[((mid[1] & 0xF0) >> 4) | 16 * (mid[0] & 3)];
      *(Dst + j++) = alpha[((mid[2] & 0xC0) >> 6) | 4 * (mid[1] & 0xF)];
      *(Dst + j++) = alpha[mid[2] & 0x3F];
    }
  }
  *(Dst + j) = 0;
```


歪攵倰政迍敶绊吓

alpha呢'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/='

受玾呢尌辙八皊flag毕3体叡或4体 + 纯俭胐炴瞉熥 -

莱专呢base64 -

+ alpha皊毕厂体恶妃呢鄗呢64迡劫敶= 3叡4乏呢base64缜砐皊笋厂岠攓佢 -

文本	M								a								n							
ASCII编码	77								97								110							
二进制位	0	1	0	0	1	1	0	1	0	1	1	0	0	0	0	1	0	1	1	0	1	1	1	0
索引	19								22								5							
Base64编码	T								W								F							

在此例中，Base64算法将三个字符编码为4个字符

+ base64皊杕贮呢3捨4幼弛搁二64迡劫 -

统刀篦匝釆吪皊劦富刃敶皊兹锴鄘刐

```
while ( len > 0 )
      {
        mid[2] = 0;
        mid[1] = 0;
        mid[0] = 0;
        for ( i = 0; i < 3 && len > 0; ++i )
        {
          mid[i] = *str1;
          --len1;
          ++str1;
        }
        if ( i ==0 )
          break;
        if ( i == 1 )
        {
          *(Dst + j++) = base[mid[0]/4];
          *(Dst + j++) = base[(mid[1]/16)|16*(mid[0]%3)];
          *(Dst + j++) = '=';
          *(Dst + j++) = '=';
        }
        else if ( i == 2 )
        {
          *(Dst + j++) = base[mid[0]/4];
          *(Dst + j++) = base[(mid[1]/16)|16*(mid[0]%3)];
          *(Dst + j++) = base[(mid[2]/64)|4*(mid[1]%15)];
          *(Dst + j++) = '=';
        }
        else if ( i == 3 )
        {
          *(Dst + j++) = base[mid[0]/4];
          *(Dst + j++) = base[(mid[1]/16)|16*(mid[0]%3)];
          *(Dst + j++) = base[(mid[2]/64)|4*(mid[1]%15)];
          *(Dst + j++) = base[mid[2]%63];
        }
      }
```


丐脡杁侣借{

```
cfr='e3nifIH9b_C@n@dH'
#alpha='ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/='
midcfr=''
#pilot
for i in range(len(cfr)):
    midcfr+=chr(ord(cfr[i])-i)
#print midcfr & midcfr='e2lfbDB2ZV95b3V9'
#base64!
import base64
plaintext=base64.b64decode(midcfr)
print plaintext
```

勰吨骒调厂丑= 稔底辙刀x

right flag{